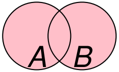
Contents

Section outline

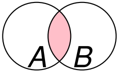
1. **Discrete structures**
   - Sets
   - Relations
   - Lattices
   - Lattices (contd.)
   - Boolean lattice
   - Boolean lattice structure
   - Boolean algebra
   - Additional Boolean algebra properties

Sets

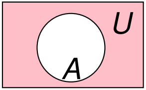
- A set A of elements: $A = \{a, b, c\}$
- Natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ or $\{1, 2, 3, \ldots\} = \mathbb{Z}^+$
- Integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Universal set: U Empty set: $\varnothing = \{\}$
- $S = \{X | X \notin X\}$ $S \in S$? [Russell's paradox]
- Set union: $A \cup B$



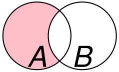
- Set intersection: $A \cap B$



- Complement: $\overline{S}$

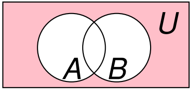


- Set difference: $A - B = A \cap \overline{B}$

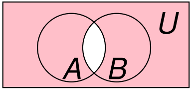


Sets (contd.)

- Complement of union (De Morgan): $\overline{A \cup B} = \overline{A} \cap \overline{B}$



- Complement of intersection (De Morgan): $\overline{A \cap B} = \overline{A} \cup \overline{B}$



- Power set of A: $\mathcal{P}(A)$

  $\mathcal{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$

- Non-empty $X_1, \ldots, X_k$ is a partition of A if $A = X_1 \cup \ldots \cup X_k$ and $X_\imath \cap X_\jmath = \varnothing \,|_{\imath \neq j}$

  $A \cap \overline{B}$, $B \cap \overline{A}$, $A \cap B$ and $\overline{A \cup B}$ constitute a partition of U

Set algebra

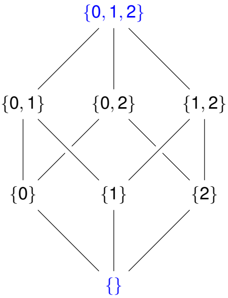
Idempotence	$A \cup A = A$	$A \cap A = A$
Associativity	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cup C = A \cap (B \cup C)$
Commutativity	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity	$A \cup \{\} = A, A \cup U = U$	$A \cap \{\} = \{\}, A \cup U = A$
Involution	$\bar{\bar{A}} = A$	
Complements	$\bar{U} = \{\}, A \cup \bar{A} = U$	$\overline{\{\}} = U, A \cap \bar{A} = \{\}$
DeMorgan	$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$

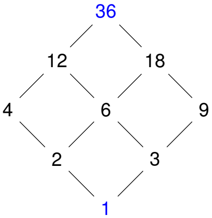
Relations

- Tuple: $\langle a, b\rangle, \langle 4, b, \alpha\rangle$
- Cartesian product: $A \times B = \{\langle a, b\rangle \mid a \in A, b \in B\}$
  $\{a, b, c\} \times \{\alpha, \beta\} = \{\langle a, \alpha\rangle, \langle b, \alpha\rangle, \langle c, \alpha\rangle, \langle a, \beta\rangle, \langle b, \beta\rangle, \langle c, \beta\rangle\}$
  $\mathbb{N} \times \mathbb{N} = \{\langle \imath, \jmath\rangle \mid \imath, \jmath \geq 1\}$
- Binary relation $\mathcal{R}$ on sets A and B: $R \subseteq A \times B$
- Characteristic function of $\mathcal{R}$: $\chi_{\mathcal{R}}(a, b) = \begin{cases} 1 & \text{if } \langle a, b\rangle \in \mathcal{R} \\ 0 & \text{if } \langle a, b\rangle \notin \mathcal{R} \end{cases}$
- $\mathcal{R} \subseteq A \times A$ is reflexive if $\forall x \in A.\ x\mathcal{R}x$
- $\mathcal{R} \subseteq A \times A$ is symmetric if $\forall x, y \in A.\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- $\mathcal{R} \subseteq A \times A$ is transitive if $\forall x, y, z \in A.\ x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$
- $\mathcal{R} \subseteq A \times A$ is antisymmetric if $\forall x, y \in A.\ x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y$
- Equivalence relation: $\mathcal{R}$ is reflexive, symmetric and transitive
- An equivalence relation induces a partition and vice versa
- Partial order: $\mathcal{R}$ is reflexive, antisymmetric and transitive

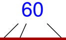
Relations (contd.)

- Connected relation: $\forall x, y \in A$, either $x\mathcal{R}y$ or $y\mathcal{R}x$
- Total order: Connected partial order (eg $\preceq$ on $\mathbb{R}$)
- Irreflexive relation: $\forall x \in A, \langle x, x\rangle \notin \mathcal{R}$
- Asymmetric relation: $\langle x, y\rangle \in \mathcal{R} \Rightarrow \langle y, x\rangle \notin \mathcal{R}$
- Strict order: $\mathcal{R}$ is irreflexive and transitive ($\therefore$ asymmetric)
- If $\preceq$ is a PO on A, then $<$: $x < y \equiv x \preceq y \wedge x \neq y$ is a SO on A
- If $<$ is a SO on A, then $\preceq$: $x \preceq y \equiv x < y \vee x = y$ is a PO on A





Divisors of 36 (60?)



Suppose $\langle A, \preceq\rangle$ is a poset, $M \in A$ ($m \in A$), $S \subseteq A$

M (m) is a maximal (minimal) element of S iff $M \in S$ ($m \in S$) and $\nexists x \in S$ st $M < x$ ($x < m$)

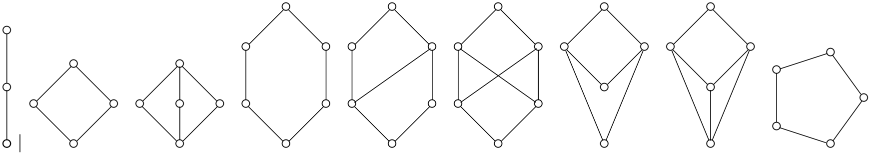
M (m) is a maximum (minimum)

Lattices

Let $\langle A, \preceq \rangle$ be a poset, let $x, y \in A$

- The *meet* of x and y ($x \wedge y$), is the maximum of all lower bounds for x and y: $x \wedge y = \max \{w \in A : w \preceq x, w \preceq y\}$, *glb* for x and y
- The *join* of x and y ($x \vee y$), is the minimum of all upper bounds for x and y; $x \vee y = \min \{z \in A : x \preceq z, y \preceq z\}$, *lub* for x and y

A poset $\langle A, \preceq \rangle$ is a lattice iff every pair of elements in A have both a meet and a join



Lattices (contd.)

Basic order properties of meet and join

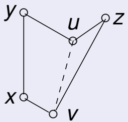
- $x \wedge y \preceq \{x, y\} \preceq x \vee y$
- $x \preceq y$ iff $x \wedge y = x$
- $x \preceq y$ iff $x \vee y = y$
- If $x \preceq y$, then $x \wedge z \preceq y \wedge z$ and $x \vee z \preceq y \vee z$
- If $x \preceq y$ and $z \preceq w$, then $x \wedge z \preceq y \wedge w$ and $x \vee z \preceq y \vee w$

Theorem

If $x \preceq y$, then $x \wedge z \preceq y \wedge z$ and $x \vee z \preceq y \vee z$

Proof.

- Let $v = x \wedge z$ and $u = y \wedge z$
- By transitivity, v is a lb for y and z
- By definition of $\wedge$, $v \preceq u$ (as u is the maximum among all lbs)



Similarly, the other clause may be proven □

Lattices (contd.)

Commutativity $x \wedge y = y \wedge x, \quad x \vee y = y \vee x$

Associativity $(x \wedge y) \wedge z = x \wedge (y \wedge z), \quad (x \vee y) \vee z = x \vee (y \vee z)$

Absorption $x \wedge (x \vee y) = x, \quad x \vee (x \wedge y) = x$

Idempotence $x \wedge x = x, \quad x \vee x = x$

Associativity of meet.

- $(x \wedge y) \wedge z \preceq x \wedge y \preceq x$ [$x \wedge y \preceq \{x, y\}$ applied twice]
- $(x \wedge y) \wedge z \preceq x$ [transitivity of $\preceq$]
- $(x \wedge y) \preceq y$ [$x \wedge y \preceq \{x, y\}$]
- $(x \wedge y) \wedge z \preceq y \wedge z$ [If $x \preceq y$, then $x \wedge z \preceq y \wedge z$]
- Thus $(x \wedge y) \wedge z$ is a lb of both x and $y \wedge z$

$\therefore$ $(x \wedge y) \wedge z \preceq x \wedge (y \wedge z)$ [glb of x and $y \wedge z$]

- Also, $x \wedge (y \wedge z) \preceq (x \wedge y) \wedge z$ [on similar lines]

$\therefore$ $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ [if $a \preceq b$ and $b \preceq a$ then $a = b$] $\square$

Lattices (contd.)

Absorbtion.

- $x \preceq x \vee y$ $[\{x, y\} \preceq x \vee y]$

$\therefore$ $x \wedge (x \vee y) = x$ $[x \preceq y$ iff $x \wedge y = x]$ $\square$

Idempotence.

- $x \wedge x = x \wedge (x \vee (x \wedge y)) = x$ [Absorbtion, applied twice] $\square$

Principle of Duality

The dual of any theorem in a lattice is also a theorem.

Lattices (contd.)

Bounded lattice: It has a maximum element (1) and a minimum element (0), in which case identity properties hold:

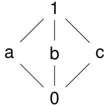
- $0 \vee x = x = x \vee 0, \quad 1 \wedge x = x = x \wedge 1$
- $0 \wedge x = 0 = x \wedge 0, \quad 1 \vee x = 1 = x \vee 1$

Every finite lattice is bounded

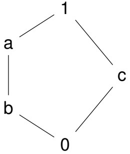
Distributive lattice: If $\forall x, y, z \in A$,

- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and
- $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

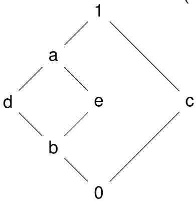
Are these lattices distributive?



$a \wedge (b \vee c) = a$
$(a \wedge b) \vee (a \wedge c) = 0$



$a \wedge (b \vee c) = a$
$(a \wedge b) \vee (a \wedge c) = b$



$a \wedge (b \vee c) = a \quad (a \wedge b) \vee (a \wedge c) = b$

Is $\mathcal{P}(A)$ for set A distributive?

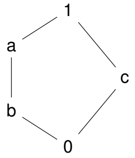
? $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$ and

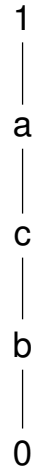
? $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$

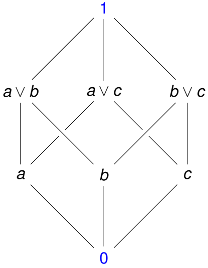
Complemented lattice

- *Complement in a bounded lattice:* z is the complement of x iff
  - $x \wedge z = 0$ and
  - $x \vee z = 1$
- **Bounded complemented lattice:** every element has a complement
- In a bounded distributive lattice with minimum 0 and maximum 1, the complements of elements are unique, provided they exist – let $\bar{x}$ and z be complements of x ...

- $\bar{x} = \bar{x} \wedge 1 = \bar{x} \wedge (x \vee z) =$
- $(\bar{x} \wedge x) \vee (\bar{x} \wedge z) =$
- $0 \vee (\bar{x} \wedge z) =$
- $(x \wedge z) \vee (\bar{x} \wedge z) =$
- $(x \vee \bar{x}) \wedge z = 1 \wedge z = z$







Boolean lattice

Boolean lattice: Bounded complemented distributive lattice

- Extreme elements: Max: 1, Min: 0
- Distributivity holds
- Every element has unique complement
- De Morgan's laws apply

De Morgan's laws in a Boolean lattice $\langle \mathcal{A}, \preceq, \bar{\ }, 0, 1\rangle$

1. $\overline{x \wedge y} = \overline{x} \vee \overline{y}$
2. $\overline{x \vee y} = \overline{x} \wedge \overline{y}$

Meet of complements is 0

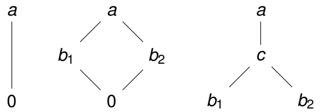
- $(x \wedge y) \wedge (\overline{x} \vee \overline{y}) = (x \wedge y \wedge \overline{x}) \vee (x \wedge y \wedge \overline{y})$
- $= 0 \vee 0 = 0$

Join of complements is 1

- $(x \wedge y) \vee (\overline{x} \vee \overline{y}) = ((x \wedge y) \vee \overline{x}) \vee \overline{y}$
- $= ((x \vee \overline{x}) \wedge (y \vee \overline{x})) \vee \overline{y}$
- $= (1 \wedge (y \vee \overline{x})) \vee \overline{y}$
- $= (y \vee \overline{x}) \vee \overline{y}$
- $= \overline{x} \vee (y \vee \overline{y})$
- $= \overline{x} \vee 1 = 1$

Boolean lattice structure

- Let $\mathcal{A}$ be a lattice with min 0
- $a \in \mathcal{A}$ is join irreducible if
  $a \neq x \vee y$ for $x, y \preceq a$, alternatively
  $a = x \vee y$ implies $a = x$ or $a = y$
- 0 is join irreducible



- If $b_1 \preceq c$ and $b_2 \preceq c$ (immediate preds) of c then $c = b_1 \vee b_2$
- $a \neq 0$ is join irreducible if and only if a has a unique immediate predecessor
- Elements immediately succeeding 0 are atoms (join irreducible)
- Any element a can be expressed as the join of a set of atoms
- Not unique for non-distributive lattice (diamond lattice)
- For finite lattice $a = d_1 \vee d_2 \vee \ldots \vee d_n$, d_j are join irreducible
- $d_j = d_\imath \vee d_j$ for $d_\imath \preceq d_j$
- Any $d_\imath \preceq d_j$ can be dropped to make the join irredundant
- Unique (up to permutation) for distributive lattice

Boolean lattice representation (contd.)

Unique irredundant irreducible sum representation

- Let $a = c_1 \vee c_2 \vee \ldots \vee c_m = d_1 \vee d_2 \vee \ldots \vee d_n$
- Now, $c_\imath, d_j \preceq c_1 \vee c_2 \vee \ldots \vee c_m = d_1 \vee d_2 \vee \ldots \vee d_n$

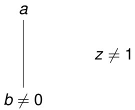
$\therefore$ $c_\imath = c_\imath \wedge (d_1 \vee d_2 \vee \ldots \vee d_n) = (c_\imath \wedge d_1) \vee (c_\imath \wedge d_2) \vee \ldots \vee (c_\imath \wedge d_n)$

- Since $c_\imath$ is join irreducible, $\exists d_j | c_\imath = c_\imath \wedge d_j$, so that $c_\imath \preceq d_j$
- But similar working, $d_j \preceq c_k$, so that $c_\imath \preceq d_j \preceq c_k$
- This requires $c_\imath = c_k$, since these are irredundant
- Thus, $c_\imath \preceq d_j$ and $d_j \preceq c_\imath$, $c_\imath = d_j$,
- This way, all the $c_\imath$s may to paired off with the d_js,

  – making the representation unique (up to permutation)

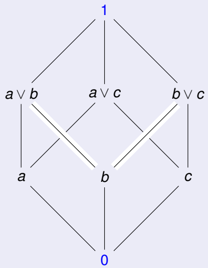
Boolean lattice structure (contd.)

- Let z be the complement of a in a lattice as shown
- So, $a \vee z = 1$ and $a \wedge z = 0$
- Suppose a has b as a unique predecessor
- Now, $b \vee z = a \vee z = 1$ and $b \wedge z = a \wedge z = 0$ as b is the immediate predecessor of a
- So, b is also a complement of z

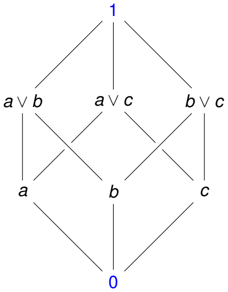


Join irreducible elements in a Boolean lattice

- A lattice with an element having a non-zero join irreducible element as a predecessor will not have unique complements
- In a Boolean lattice all non-zero join irreducible elements are atoms



Stone representation of Boolean lattices



- Atom of a Boolean lattice: Non-trivial minimal element of $A \setminus \{0\}$
- $|A| = 2^n$ for some n for a Boolean lattice
- Its structure is that of the power set of the atomic elements

- Non-trivial atomic elements are present for $|A| > 1$ directly above level 0, let those be $S = \{a_1, \ldots, a_n\}$, akin to $\{a_1\}, \{a_2\}, \ldots \{a_n\}$
- Join of pairs of elements Y_1, Y_2 at level i ($n > i > 1$) st $|Y_1 - Y_2| = |Y_2 - Y_1| = 1$ at level $\imath + 1$ is $Y = Y_1 \cup Y_2$
- Meet of pairs of elements X_1, X_2 at level $\imath$ ($n > i > 1$) st $|X_1 - X_2| = |X_2 - X_1| = 1$ at level $\imath - 1$ is $Y = Y_1 \cap Y_2$
- There will be $\binom{n}{\imath}$ such sets in level $\imath$, totaling to $\sum_{\imath=0}^{\imath=n} \binom{n}{\imath} = 2^n$

Boolean algebra from Boolean lattice

- For the Boolean lattice $\langle \mathcal{A}, \preceq, 0, 1 \rangle$ consider the algebraic system $\langle \mathcal{A}, +, \cdot, ^{-}, 0, 1 \rangle$ where $\vee \mapsto +$, $\wedge \mapsto \cdot$ and $\forall x \in \mathcal{A}$, $\overline{x} \mapsto z | x + z = 1, x \cdot z = 0$
- This system satisfies the Huntington's postulates for a Boolean algebra

B1: Commutative Laws

1. $x + y = y + x$
2. $x \cdot y = y \cdot x$

B2: Distributive Laws

1. $x \cdot (y + z) = x \cdot y + x \cdot z$
2. $x + (y \cdot z) = (x + y) \cdot (x + z)$

B3: Identity Laws

1. $x + 0 = x = 0 + x$
2. $x \cdot 1 = x = 1 \cdot x$

B4: Complementation Laws

1. $x + \bar{x} = 1 = \bar{x} + x$
2. $x \cdot \bar{x} = 0 = \bar{x} \cdot x$

Additional Boolean algebra properties

- These properties carry over from the Boolean lattice
- May be proven independently from the Huntington's postulates

Idempotence:

1. $x + x = x$
2. $x \cdot x = x$

Axiomatic proof

- $x + x = (x + x) \cdot 1$
- $= (x + x) \cdot (x + \bar{x})$
- $= x + (x \cdot \bar{x})$
- $= x + 0 = x$

Absorption:

1. $x + xy = x$
2. $x \cdot (x + y) = x$
3. $x + \bar{x}y = x + y$
4. $x \cdot (\bar{x} + y) = xy$

Axiomatic proof

- $x + xy = (x \cdot 1) + xy$
- $= x(1 + y) = x(y + 1)$
- $= x \cdot 1 = x$

Boolean algebra (contd.)

Boundedness/annihilation:

1. $x + 1 = 1$
2. $x \cdot 0 = 0$

Axiomatic proof

- $x + 1 = 1 \cdot (x + 1)$
- $= (x + \bar{x}) \cdot (x + 1)$
- $= x + (\bar{x} \cdot 1)$
- $= x + \bar{x} = 1$

Truth table for Boolean AND, OR, NOT:

x	y	$\overline{x}$	$x \cdot y$	$x + y$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

Associativity:

1. $(x + y) + z = x + (y + z)$
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

Boolean algebra (contd.)

Axiomatic proof of associativity of Boolean $+$

- Let $x = a + (b + c)$ and $y = (a + b) + c$
- $ax = aa + a(b + c) = a + a(b + c) = a$
- $bx = ba + b(b + c) = ba + (bb + bc) = ba + (b + bc) = ba + b = b$
- Similarly, $cx = c$ and $ay = a$, $by = b$ and $cy = c$
- $yx = ((a+b)+c)x = (a+b)x+cx = (ax+bx)+cx = (a+b)+c = y$
- $xy = (a+(b+c))y = ay+(b+c)y = ay+(by+cy) = a+(b+c) = x$
- Thus, $x = xy = yx = y$

Additional Boolean algebra properties (contd.)

Uniqueness of Complement:

If $(a + x) = 1$ and $(a \cdot x) = 0$, then $x = \overline{a}$.

Involution:

$$\overline{(\overline{a})} = a$$

Complements of extreme elements:

- $\overline{0} = 1$
- $\overline{1} = 0$

Axiomatic proof

- $1 + 0 = 1$ [identity]
- $1 \cdot 0 = 0$ [boundedness]

$\therefore$ 0 is the complement of 1

DeMorgan's laws:

- $\overline{(x + y)} = \overline{x} \cdot \overline{y}$
- $\overline{(x \cdot y)} = \overline{x} + \overline{y}$

- Let $a \preceq b$ if $a \cdot b = a$ or $a + b = b$ then $\cdot \mapsto \wedge$ and $+ \mapsto \vee$
- Properties from axiomatic proofs allow Boolean algebras to be expressed as Boolean lattices – they are equivalent